1/5/1 (Item 1 from file: 351)
DIALOG(R)File 351:DERWENT WPI

011449711 **Image available**
WPI Acc No: 97-427618/199740
XRPX Acc No: N97-355924
Data compression and encryption processing and strength of cryptanalysis - generating random number and different key for each data on random number, setting work key and feeding back pre-encrypted result to frequently change work key
Patent Assignee: HITACHI LTD (HITA); HITACHI SEISAKUSHO KK (HITA)
Inventor: SHIMIZU M; TAKARAGI K; YOSHIURA H
Number of Countries: 007 Number of Patents: 006
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
EP 793366	A2	19970903	EP 97103154	A	19970226	H04L-009/06	199740 B
AU 9714952	A	19970918	AU 9714952	A	19970227	H04L-009/16	199746
JP 9230786	A	19970905	JP 9640931	A	19960228	G09C-001/00	199746
AU 693733	B	19980702	AU 9714952	A	19970227	H04L-009/16	199837
KR 97064059	A	19970912	KR 974889	A	19970218	H04L-009/00	199840
AU 9887869	A	19981126	AU 9714952	A	19970227	H04L-009/16	199908
			AU 9887869	A	19981002		

Priority Applications (No Type Date): JP 9640931 A 19960228
Cited Patents: No-SR.Pub
Patent Details:

Patent	Kind	Lan	Pg	Filing Notes	Application	Patent
EP 793366	A2	E	18			
Designated States (Regional): DE FR GB SE						
JP 9230786	A		9			
AU 693733	B			Previous Publ.		AU 9714952
AU 9887869	A			Div ex	AU 9714952	

Abstract (Basic): EP 793366 A
The information processing method (10) involves entering or receiving data. A parameter (116) is provided for encrypting a portion of the data, using an intermediate result given in the process of encrypting another portion of the data or a value derived on the intermediate result. The data is encrypted using the parameter.
Preferably The data is divided into several blocks. The blocks are sequentially encrypted through the encryption process. The parameter for encrypting one of the blocks is an intermediate result given in the process of encrypting one or more blocks previous to the block or a value derived on the intermediate result. Each of the blocks is encrypted using the parameter to encrypt the data.
USE/ADVANTAGE - Improves processing performance and security of cryptosystem without increasing processing time.
Dwg.1/6
Title Terms: DATA; COMPRESS; ENCRYPTION; PROCESS; STRENGTH; GENERATE; RANDOM; NUMBER; KEY; DATA; RANDOM; NUMBER; SET; WORK; KEY; FEED; BACK; PRE; ENCRYPTION; RESULT; FREQUENT; CHANGE; WORK; KEY
Derwent Class: P85; W01
International Patent Class (Main): G09C-001/00; H04L-009/00; H04L-009/06; H04L-009/16
International Patent Class (Additional): H03M-007/30
File Segment: EPI; EngPI

1/5/2 (Item 1 from file: 347)
DIALOG(R)File 347:JAPIO

05615986 **Image available**
ENCODING METHOD OF DATA AND DEVICE THEREFOR

PUB. NO.: 09-230786 **JP 9230786** A]
PUBLISHED: September 05, 1997 (19970905)
INVENTOR(s): YOSHIURA YUTAKA
TAKARAGI KAZUO
SHIMIZU MAYUKO
APPLICANT(s): HITACHI LTD [000510] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 08-040931 [JP 9640931]
FILED: February 28, 1996 (19960228)
INTL CLASS: [6] G09C-001/00; G09C-001/00; H03M-007/30; H04L-009/16
JAPIO CLASS: 44.9 (COMMUNICATION -- Other); 42.4 (ELECTRONICS -- Basic Circuits); 44.3 (COMMUNICATION -- Telegraphy)

ABSTRACT

PROBLEM TO BE SOLVED: To achieve a code strength that endures the latest decoding technique (difference decoding and linear decoding) without accompanied by an increase in processing time in data compression and encoding

SOLUTION: In a difference and linear decoding, two or more pairs of ordinary and ciphered sentences to same key are collected and the key is presumed by a statistical processing. Here, when ordinary sentence (111) data are inputted to an I/O processor (102), it generates random numbers (104), and forms (105) and a different key to each data based on the random numbers and the keys are defined as executing keys (115). Also, an intermediate result of the encoding, namely, precoding (118) are fed back and the executing keys are repeatedly modified. From the above, the difference and linear decodings can be prevented. Further, based on the executing keys, compression (107) is provided with encoding function by altering (106) a corresponding relationship (114) between an ordinary sentence and a compressed sentence in compression (107). Thus, a code strength is further improved.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平9－230786

(43)公開日　平成９年(1997)９月５日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０９Ｃ	1/00	６１０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６１０Ａ
		６３０	7259－5Ｊ			６３０Ｚ
Ｈ０３Ｍ	7/30		9382－5Ｋ	Ｈ０３Ｍ	7/30	Ｚ
Ｈ０４Ｌ	9/16			Ｈ０４Ｌ	9/00	６４３

審査請求　未請求　請求項の数25　ＯＬ　（全９頁）

(21)出願番号　特願平8－40931

(22)出願日　平成８年(1996)２月28日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　吉浦　裕
神奈川県川崎市麻生区王禅寺1099番地株式会社日立製作所システム開発研究所内

(72)発明者　宝木　和夫
神奈川県川崎市麻生区王禅寺1099番地株式会社日立製作所システム開発研究所内

(72)発明者　清水　麻由子
神奈川県横浜市戸塚区戸塚町5030番地株式会社日立製作所ソフトウェア開発本部内

(74)代理人　弁理士　小川　勝男

(54)【発明の名称】　データの暗号化方法及び装置

(57)【要約】

【課題】データの圧縮・暗号化において、処理時間の増加を伴わずに最新の暗号解読手法（差分解読および線形解読）に耐える暗号強度を達成する。

【解決手段】差分及び線形解読では、同じ鍵に対する平文と暗号の対を複数収集し、統計処理により鍵を推定する。そこで、入出力処理（１０２）が平文データ（１１１）を入力すると、乱数を発生し（１０４）、その乱数に基づいてデータ毎に異なる鍵を生成し（１０５）、これを実行鍵（１１５）とする。また、暗号化の中間結果すなわち前段暗号化（１０８）の結果をフィードバックして実行鍵（１１５）を頻繁に変更する。以上により、差分及び線形解読を防止できる。また、実行鍵に基づいて、圧縮（１０７）における平文と圧縮文の対応関係（１１４）を変更する（１０６）ことにより、圧縮を暗号機能を持たせる。その結果、暗号強度をさらに向上することができる。

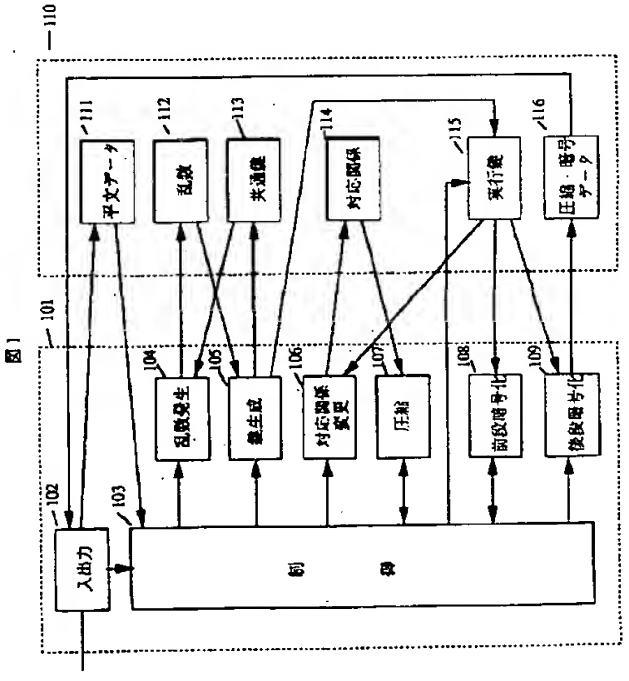


図１

1

【特許請求の範囲】

【請求項１】データを入力または受信するステップと、そのデータを暗号化するステップを有する情報処理システムにおいて、

データのある部分の暗号化のパラメータとして、データの他の部分の暗号化の中間結果あるいはこの中間結果に依存して算出した値を用いることを特徴とするデータの暗号化方法。

【請求項２】データを入力または受信するステップと、そのデータを暗号化するステップと、データを複数のブロックに分割し、上記暗号化ステップを用いて上記ブロックを順次暗号化するステップを有する情報処理システムにおいて、

あるブロックの暗号化のパラメータとして、そのブロックより以前に暗号化した一つ以上のブロックの暗号化の中間結果あるいはこれらの中間結果に依存して算出した値を用いることを特徴とするデータの暗号化方法。

【請求項３】データを入力または受信するステップと、そのデータを暗号化するステップと、データを複数のブロックに分割し、上記暗号化ステップを用いて上記ブロックを並列に暗号化するステップを有する情報処理システムにおいて、

処理のある時点におけるあるブロックの暗号化のパラメータとして、そのブロック以外の一つ以上のブロックの暗号化の中間結果のうち、その時点において算出済みのもの、あるいはこれらの算出済み中間結果に依存して算出した値を用いることを特徴とするデータの暗号化方法。

【請求項４】データを入力または受信するステップと、そのデータを圧縮するステップと、圧縮されたデータを暗号化するステップを有する情報処理システムにおいて、

データのある部分の圧縮における入力データ中のビット列と圧縮データ中のビット列の対応関係を、データの他の部分の暗号化の中間結果に依存して決定することを特徴とするデータの暗号化方法。

【請求項５】データを入力または受信するステップと、そのデータを圧縮するステップと、圧縮されたデータを暗号化するステップと、データを複数のブロックに分割し、上記圧縮ステップと暗号化ステップを用いて上記ブロックを順次圧縮かつ暗号化するステップを有する情報処理システムにおいて、

あるブロックの圧縮における入力データ中のビット列と圧縮データ中のビット列の対応関係を、そのブロックより以前に圧縮かつ暗号化した一つ以上のブロックの暗号化の中間結果に依存して決定することを特徴とするデータの暗号化方法。

【請求項６】データを入力または受信するステップと、そのデータを圧縮するステップと、圧縮されたデータを暗号化するステップと、データを複数のブロックに分割し、上記圧縮ステップと暗号化ステップを用いて上記ブロックを並列に圧縮かつ暗号化するステップを有する情報処理システムにおいて、

処理のある時点において、あるブロックの圧縮における入力データ中のビット列と圧縮データ中のビット列の対応関係を、そのブロック以外の一つ以上のブロックの暗号化の中間結果のうち、その時点において算出済みのものに依存して決定することを特徴とするデータの暗号化方法。

【請求項７】請求項１又は請求項２又は請求項３又は請求項４又は請求項５又は請求項６記載の暗号化方法において、

上記暗号化ステップがｎ個の複数の処理から構成され、ｍ１、ｍ２、・・・ｍｋがそれぞれ１以上ｎ以下の整数であり、前記暗号化の中間結果が、ｍ１番目の処理の結果，ｍ２番目の処理の結果，・・・ｍｋ番目の処理の結果であることを特徴とするデータの暗号化方法。

【請求項８】請求項１又は請求項２又は請求項３又は請求項４又は請求項５又は請求項６又は請求項７記載の暗号化方法において、

処理のある時点で、暗号化のパラメータあるいは、入力データ中のビット列と圧縮データ中のビット列の対応関係を上記暗号化の中間結果に依存しない値に変更することを特徴とするデータの暗号化方法。

【請求項９】データを入力または受信するステップと、そのデータを暗号化するステップを有する情報処理システムにおいて、

乱数を発生し、その乱数あるいはそれに依存して算出された値を上記データの暗号化のパラメータとすることを特徴とするデータの暗号化方法。

【請求項１０】請求項９記載の暗号化方法において、

初期値に対して暗号化処理を繰り返し適用することにより上記乱数を発生することを特徴とするデータの暗号化方法。

【請求項１１】請求項９又は請求項１０記載の暗号化法において、

上記乱数発生ステップを複数回実行することにより複数の乱数を求め、それらを上記データの異なる部分の暗号化のパラメータとすることを特徴とするデータ暗号化方法。

【請求項１２】請求項９又は請求項１０又は請求項１１記載の暗号化方法において、

上記データの暗号化のパラメータあるいはその値の算出に必要な情報を、データの暗号結果に付加することを特徴とするデータの暗号化方法。

【請求項１３】請求項９又は請求項１０又は請求項１１又は請求項１２記載の暗号化方法において、

上記暗号化されたデータの復号化において、上記データの暗号化のパラメータあるいはその値の算出に必要な情報を用いることを特徴とするデータの暗号化方法。

【請求項１４】請求項１３記載の暗号化方法において、上記データの暗号化ステップを実行する計算機と上記データの復号化ステップを実行する計算機が異なっており、暗号化ステップを実行する計算機から復号化ステップを実行する計算機に、上記データの暗号化のパラメータあるいはその値の算出に必要な情報を通信することを特徴とするデータの暗号化方法。

【請求項１５】データを入力または受信する手段と、そのデータを暗号化する手段を有する情報処理装置において、

上記暗号化手段における暗号化の中間結果を記憶する手段と、上記記憶した中間結果あるいはこの中間結果に依存した値を上記暗号化手段にパラメータとして入力する手段を有することを特徴とするデータの暗号化装置。

【請求項１６】データを入力または受信する手段と、データを暗号化する複数の手段を有する情報処理装置において、

上記暗号化手段における暗号化の中間結果を、上記の他の暗号化手段にパラメータとして入力する手段を有することを特徴とするデータの暗号化装置。

【請求項１７】データを入力する手段と、データを圧縮する手段と、データを暗号化する手段を有する情報処理装置において、

上記暗号化手段における暗号化の中間結果を記憶する手段と、上記記憶した中間結果あるいはこの中間結果に依存した値を上記圧縮手段にパラメータとして入力する手段を有することを特徴とするデータの暗号化装置。

【請求項１８】データを入力または受信する手段と、データを圧縮する手段およびデータを暗号化する手段の複数の対を有する情報処理装置において、

上記の対の暗号化手段における暗号化の中間結果を、上記の他の対の圧縮手段にパラメータとして入力する手段を有することを特徴とするデータの暗号化装置。

【請求項１９】請求項１５又は請求項１６又は請求項１７記載の暗号化装置および圧縮・暗号化装置において、

上記暗号化の中間結果を記憶する手段において記憶されている値を、暗号化の中間結果に依存しない値に変更する手段を有することを特徴とするデータの暗号化装置。

【請求項２０】請求項１５又は請求項１６又は請求項１７又は請求項１８記載の暗号化装置および圧縮・暗号化装置において、

暗号化の中間結果に依存しない値を算出あるいは記憶する手段と、その値を上記暗号化手段または圧縮手段にパラメータとして入力する手段を有することを特徴とするデータの暗号化装置。

【請求項２１】データを入力または受信する手段と、そのデータを暗号化する手段を有する情報処理装置において、

乱数を発生する手段と、上記乱数あるいはこの乱数に依存した値を上記暗号化手段にパラメータとして入力する

手段を有することを特徴とするデータの暗号化装置。

【請求項２２】データを入力または受信する手段と、そのデータを暗号化する手段を有する情報処理装置において、

記憶された値を暗号化する第２の暗号化手段と、上記第２の暗号化手段の出力値あるいはこの出力値に依存した値を上記第１の暗号化手段にパラメータとして入力する手段と、上記第２の暗号化手段の出力値を記憶する手段を有することを特徴とするデータの暗号化装置。

【請求項２３】請求項２１又は請求項２２記載の暗号化装置において、

上記パラメータあるいはその値の算出に必要な情報を、上記第１の暗号化の出力値に付加する手段を有することを特徴とするデータの暗号化装置。

【請求項２４】請求項２１又は請求項２２又は請求項２３記載のの暗号化装置において、

上記パラメータあるいはその値の算出に必要な情報を用いてデータを復号する手段を有することを特徴とするデータの暗号化装置。

【請求項２５】請求項２４記載の暗号化装置において、

上記第１および第２の暗号化手段と、上記復号化手段が異なる計算機上にあり、暗号化手段を有する計算機が上記パラメータあるいはその値の算出に必要な情報を送信する手段を有し、復号化手段を有する計算機がパラメータあるいはその値の算出に必要な情報を受信する手段を有することを特徴とするデータの暗号化装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、データの暗号化に関し、特に暗号化における処理効率および解読に対する強度の向上に関する。また、本発明は、データの圧縮を含む暗号化に関し、特に、データに圧縮と暗号化の両方を施す暗号化の処理効率および解読に対する強度の向上に関する。

【０００２】

【従来の技術】組織の中枢情報が電子化され、かつ、ネットワークを介して通信されることが増えるに従い、電子化されたデータを盗み見および改竄から守るために、データ暗号化技術の重要性が高まっている。暗号理論入門、共立出版（１９９３年）、２７頁から３２頁に述べられているように、暗号方式は、対称暗号と非対称鍵暗号に大きく分けられるが、本発明では、大量データの暗号化に適した対称暗号の改良を目的とする。以下、秘密鍵暗号を単に暗号と呼ぶことにする。

【０００３】まず、暗号に関する基本的な用語を説明する。上記文献の３３頁から５９頁に述べられているように、暗号では、秘密のパラメータを用いて平文データを暗号データに変換する。暗号データの復号では、暗号化に用いたのと同じ秘密のパラメータを用いた逆変換により、元の平文データを求める。この秘密のパラメータ

を、一般に暗号の鍵と呼ぶ。また、暗号処理は、一種類あるいは数種類の基本関数の繰り返しから構成される。この繰り返しの回数を暗号の段数と呼ぶ。また、暗号処理の利用にあたっては、入力データを所定サイズの部分に分割し、部分毎に暗号処理を適用する。この処理の単位となるデータを暗号のブロックと呼ぶ。

【０００４】暗号の方式設計及び運用では、各種の暗号解読方法に対する防御が重要な要件となる。従来最も多く用いられている解読方法は鍵の全数探索であるが、最近では、より効率的な差分解読および線形解読が注目されている。

【０００５】上記文献の１６３頁から１６６頁、および、DES暗号の線形解読法、暗号と情報セキュリティシンポジウム（１９９３年）に述べられているように、差分および線形解読では、暗号方式に固有の平文データ、暗号データ、鍵の間の相関を利用し、同じ鍵による暗号処理の入出力（平文データと暗号データ）を多数収集して、統計処理を行うことによりその鍵を推定する。

【０００６】従来の暗号方式における差分及び線形解読への防御方法は、暗号段数の増加により、平文データ、暗号データ、鍵の間の相関を小さくする方法であった。

【０００７】

【発明が解決しようとする課題】暗号および復号の処理時間は、暗号段数に比例する。そこで、上記暗号段数の増加による差分及び線形解読への防御には、処理時間の増加という大きな問題があった。本発明が解決しようとする課題は、処理時間の増加を伴わずに、差分及び線形解読を防止する方法を確立することにより、暗号における処理性能とセキュリティを向上させることである。

【０００８】

【課題を解決するための手段】上述したように、差分及び線形解読では、同じ鍵による暗号処理の入出力（平文データと暗号データ）を多数収集して、統計処理を行うことにより鍵を推定する。そこで、本発明の第１の方法では、平文データを入力または受信するステップと、そのデータを暗号化するステップを有する情報処理システムにおいて、平文データのあるブロックの暗号化の鍵として、他のブロックの暗号化の中間結果あるいはそれに依存して算出した値を用いる。本方法によると、平文データに依存してブロック毎に鍵が異なるので、上記の統計処理が不可能となり、差分および線形解読を防止できる。

【０００９】上記第１の方法では、平文データのうち最初に暗号化されるブロックについては、他のブロックの暗号化の中間結果が利用できないので、鍵が一定となる。そこで、多数の平文データに亘って最初のブロックの入出力を収集することにより、最初のブロックの鍵が推定され、それを手掛りに暗号全体が解読される可能性がある。この問題を解決するために、本発明の第２の方法では、平文データを入力または受信するステップと、

そのデータを暗号化するステップを有する情報処理システムにおいて、平文データ毎に乱数を発生し、その値をその平文データの暗号化における最初のブロックの鍵とする。この第２の方法によれば、平文データ毎に最初のブロックの鍵が異なるので、上記の第１の方法の問題点を解決できる。

【００１０】また、暗号処理は、圧縮処理と共に利用される場合が多い。データ圧縮ハンドブック、トッパン（１９９４年）、２１頁から２４７頁に述べられているように、圧縮では、平文データのビット列をより短いビット列に置き換えることによりデータを圧縮するが、平文データのビット列と圧縮データのビット列の対応関係は複数通り可能である。そこで、本発明の第３の方法では、データを入力または受信するステップと、そのデータを圧縮するステップと、圧縮データを暗号化するステップを有する情報処理システムにおいて、平文データのあるブロックの圧縮における平文データのビット列と圧縮データのビット列の対応関係を、他のブロックの暗号化の中間結果に依存して決定する。この第３の方法によれば、平文データのビット列と圧縮データのビット列の対応関係が、平文データに依存してブロック毎に変わる。また、暗号化の中間結果は、鍵を知らない限り推定不能であるので、平文データのビット列と圧縮データのビット列の対応関係の変化は鍵を知らない限り推定不能である。従って、上記第３の方法によれば、圧縮を一種の暗号とすることができ、暗号段数を増加するのと同様の効果が得られ、差分及び線形解読を防止できる。

【００１１】

【発明の実施の形態】以下の図１～図４を用いて本発明の一実施例を説明する。

【００１２】図１は、本発明のソフトウェア構成を示す。ブロック１０１は処理であり、入出力１０２、制御１０３、乱数発生１０４、鍵生成１０５、対応関係変更１０６、圧縮１０７、前段暗号化１０８、後段暗号化１０９から成る。ブロック１１０はメモリであり、平文データ１１１、乱数１１２、共通鍵１１３、対応関係１１４、実行鍵１１５、圧縮・暗号データ１１６を記憶する。

【００１３】入出力１０２は、外部から平文データを入力し、メモリ１１０に格納する。また、圧縮・暗号命令を入力し、制御１０３に渡す。一方、圧縮・暗号データ１１６をメモリ１１０から読み出し、外部に出力する。制御１０３は、入出力１０２から圧縮・暗号命令を受け取ったときに、乱数発生１０４を起動して乱数を発生し、次に、鍵生成１０５を起動して実行鍵を生成する。次に、平文データ１１１をメモリ１１０から読み出し、圧縮１０７、前段暗号化１０８、後段暗号化１０９、対応関係変更１０６、実行鍵の変更の５つの処理を繰返し実行することにより、平文データを圧縮・暗号化する。制御１０３については、後に詳述する。

【００１４】乱数発生１０４の実現には、暗号理論入門、共立出版（１９９３年）、６１頁から８６頁に述べられているような従来の乱数発生方法を用いる。一例としては、メモリ１１０中の乱数１１２に適当な初期値を設定しておき、乱数発生１０４が起動される毎に、前回の乱数１１２を読み出し、これに乱数発生１０４の内部で暗号処理を適用し、その結果を新たな乱数とする。また、メモリ１１０中の乱数１１２を新たな乱数で置き換える。

【００１５】鍵生成１０５は、乱数１１２と共通鍵１１３から実行鍵１１５を生成する。その実現には、電子情報通信学会論文誌、Ｅ７４巻、８号、２１５３頁から２１５９頁(Institution for Electronic, Information and Communication Engineers, Transaction, Vol. E74, No. 8, pp.2153-2159)に述べられているような方法を用いる。

【００１６】対応関係変更１０６は、平文データ中のビット列と圧縮データ中のビット列の対応関係１１４を、実行鍵に基づいて変更する。この対応関係の具体例は、圧縮１０９の具体例に依存する。本実施例では、圧縮１０７でハフマン圧縮を用いる。ハフマン圧縮における平文ビット列と圧縮ビット列の対応関係はハフマン木と呼ばれる木構造データにより表されるので、対応関係変更１０６はこのハフマン木を変更する。対応関係変更１０６については、後に詳述する。

【００１７】圧縮１０７は、上記のようにハフマン圧縮を行う。対応関係１１４のハフマン木に従って、平文データ中のビット列を圧縮データのビット列に置き換えることにより、平文データを圧縮する。ハフマン圧縮は、データ圧縮ハンドブック、トッパン（１９９４年）、２１頁から１０３頁に述べられているような従来の方法により実現する。

【００１８】前段暗号化１０８は、実行鍵１１５をパラメータとして、暗号理論入門、共立出版（１９９３年）、３３頁から５９頁に述べられているような従来の暗号方法により、データを暗号化する。後段暗号化１０９も前段暗号化１０８と同様に、実行鍵１１５をパラメータとして、従来方法によりデータを暗号化する。

【００１９】図２は、制御１０３の動作の詳細を示す。まず、ステップ２０１は、乱数発生１０４を起動して乱数を発生する。ステップ２０２は、鍵生成１０５を起動し実行鍵を生成する。その結果、実行鍵１１５の初期値が設定される。ステップ２０３は、平文データ１１１を読み込む。

【００２０】ステップ２０４は、圧縮１０７を起動して平文データの次の記号を圧縮する。ここで圧縮１０７は、対応関係１１４に従って平文データの記号（ビット列）を圧縮ビット列に変換することにより、平文データを圧縮する。ステップ２０５は、圧縮データの量が暗号処理のブロックサイズ以上溜まったかどうかを判定する。ブロックサイズ以上溜まった場合には、ステップ２０６に進む。ブロックサイズ未満の場合にはステップ２０４を繰り返す。

【００２１】ステップ２０６は、圧縮データの１ブロックを前段暗号化１０８に入力して、これを暗号化する。ここで前段暗号化１０８は、実行鍵１１５をパラメータとして用いる。ステップ２０７は、前段暗号化１０８の結果を記憶する。ステップ２０８は、前段暗号化の結果を後段暗号化１０９に入力して、これをさらに暗号化する。ここで後段暗号化１０９は、前段暗号処理と同じく実行鍵１１５をパラメータとして用いる。また、結果の圧縮・暗号データに実行鍵を付加したデータを、圧縮・暗号データ１１６としてメモリ１１０に格納する。

【００２２】ステップ２０９は、平文データ中のビット列と圧縮データ中のビット列の対応関係１１４を、前段暗号化の結果に依存して変更する。ステップ２１０は、実行鍵１１５を前段暗号化の結果で置き換える。ステップ２１１は、平文データを全て処理したかどうかを判定する。全て処理した場合には、処理を終了する。そうでない場合には、ステップ２１２に進む。

【００２３】ステップ２１２は、所定の暗号ブロック数を処理したかどうかを判定する。処理した場合には、ステップ２０１に戻る。処理していない場合には、ステップ２０４に戻る。ステップ２０１に戻ることの意味は、以下の通りである。

【００２４】本実施例では、一つのブロックの暗号化の中間結果（前段暗号化の結果）が、次のブロックの圧縮および暗号化のパラメータとなる。本実施例の出力となる圧縮・暗号データの伸張・復元では、圧縮・暗号時と同じパラメータが必要となるので、一つのブロックの復号化の中間結果を、次のブロックの復号および伸張のパラメータとする必要がある。従って、圧縮・暗号されたデータが、通信やファイル記憶中に１ビットでも誤った場合、そのビットを含むブロックの復号化の中間結果が誤りとなり、その結果、次のブロックの復号及び伸張のパラメータが誤りとなる。この誤りは、データの最後のブロックまで伝搬する。

【００２５】近年の通信及びファイル記憶におけるエラー訂正技術の向上により、本発明の適用対象となるアプリケーション層ではエラーは殆ど起きない。従って、本発明の殆どの適用システムでは、上記のエラー伝搬は問題にならない。しかし、中にはエラー訂正を行わない応用システムもあり、それらのシステムに本発明を適用する場合には、エラー伝搬を所定のブロック数に限定する必要がある。

【００２６】上記のステップ２１２からステップ２０１への戻りは、この要求に応えるものである。すなわち所定のブロック数に達したときには、ステップ２０１、２０２により、実行鍵が前ブロックの暗号化の中間結果とは無関係な値にリセットされるので、エラー伝搬を回避

できる。

【００２７】次に、図３、４を用いて、対応関係変更１０６の動作を説明する。ハフマン圧縮では、平文データのビット列と圧縮データのビット列の対応関係１１４をハフマン木で表現する。図３は、ハフマン木の一例を示す。ハフマン木は、各中間ノードから左右の枝が出ている２分木であり、左右の枝には、０または１の値が付加されている。末端ノードは平文データの１つの記号を表す。末端ノードからルートノードまでの枝の値を連接したものが、末端ノードの表す記号に対応する圧縮データのビット列である。例えば、ｉに対応する圧縮データのビット列は１０００であり、ｈに対応する圧縮データのビット列は０１０である。

【００２８】対応関係変更１０６は制御１０３から起動される。対応関係変更１０６は、まず、ハフマン木の中間ノードに番号を付ける。具体的には、ルートノードを１番、２段目のノードを左から２番および３番、３段目のノードを左から４番、５番・・・というように、トップダウン、レフトライトの順で番号を付ける。次に、実行鍵に従って、中間ノードの左右の枝の値を入れ替える。具体的には、実行鍵のｉ番目のビットが１ならば、ｉ番目の中間ノードの左右の枝の値を入れ替える（０ならば入れ替えない）。

【００２９】図４ブロック４０１は、実行鍵が１１００１００・・・の場合の、図３からの変更後のハフマン木を示す。ブロック４０２は、実行鍵が１０１０１１０・・・の場合の、ブロック４０１からの変更後のハフマン木を示す。なお、実行鍵のビット数は十分に大きく取ることとし、実行鍵のビットのうちハフマン木の中間ノード数を越えるものは、対応関係変更１０６では無視することにする。

【００３０】以上が本発明の実施例である。従来の暗号方法では線形及び差分解読を防止するために暗号段数を増やしていたが、その防止方法には処理時間の増加という欠点があった。上記実施例によれば、実行鍵をブロック毎に変更することにより、鍵を推定するための統計処理を不可能とし、差分及び線形解読を防止できる。ブロック毎の実行鍵は、前のブロックの暗号化の中間結果なので、実行鍵を変更するための余分の処理時間は必要ない。以上から、本実施例によれば、処理時間の増加を伴わずに差分及び線形解読を防止することができ、暗号の性能及び解読に対する強度を向上できる。

【００３１】また、本実施例によれば、圧縮における平文データと圧縮データの対応関係を、前のブロックの暗号化の中間結果に依存してブロック毎に変更することができる。暗号化の中間結果は鍵を知らない限り推定不可能であるため、平文データと圧縮データの対応関係は推定不可能となる。そこで、本実施例によれば、圧縮と一種の暗号として利用することができ、暗号の段数を増加したのと同様に、差分及び線形解読を防止できる。

【００３２】

【発明の効果】暗号処理および圧縮・暗号処理において、処理時間の増加を伴わずに、差分解読および線形解読を防止できるので、上記処理の性能及び解読に対する強度を向上できる。

【図面の簡単な説明】

【図１】本発明の実施例のソフトウェア構成図である。

【図２】本発明の実施例における制御処理の動作を示すフローチャートである。

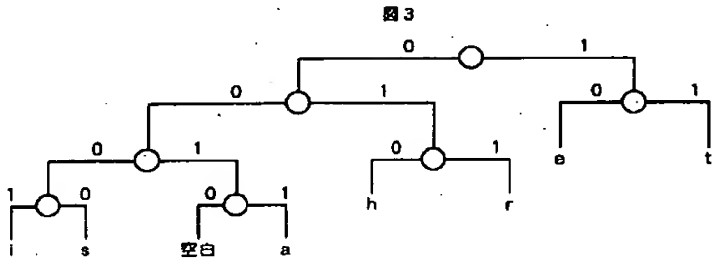
【図３】本発明の実施例における平文データと圧縮データの対応関係を示すハフマン木の例を示す図である。

【図４】本発明の実施例におけるハフマン木の変形の例を示す図である。

【符号の説明】

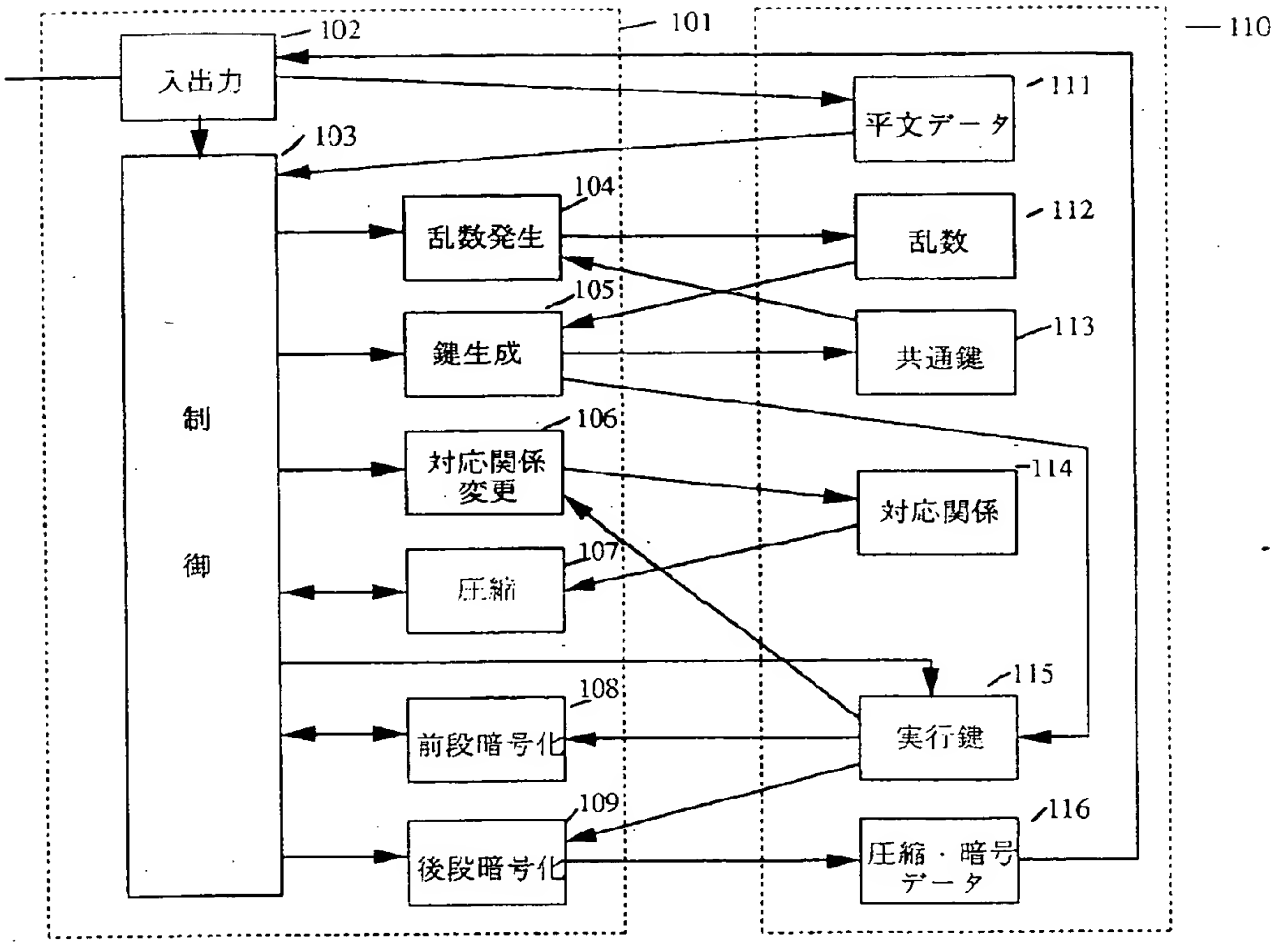
１０２…入出力処理、１０４…乱数発生処理、１０５…鍵生成処理、１０６…対応関係変更処理、１０７…圧縮処理、１０８…全段暗号化処理、１１１…平分データ、１１５…実行鍵、１１４…対応関係

【図３】

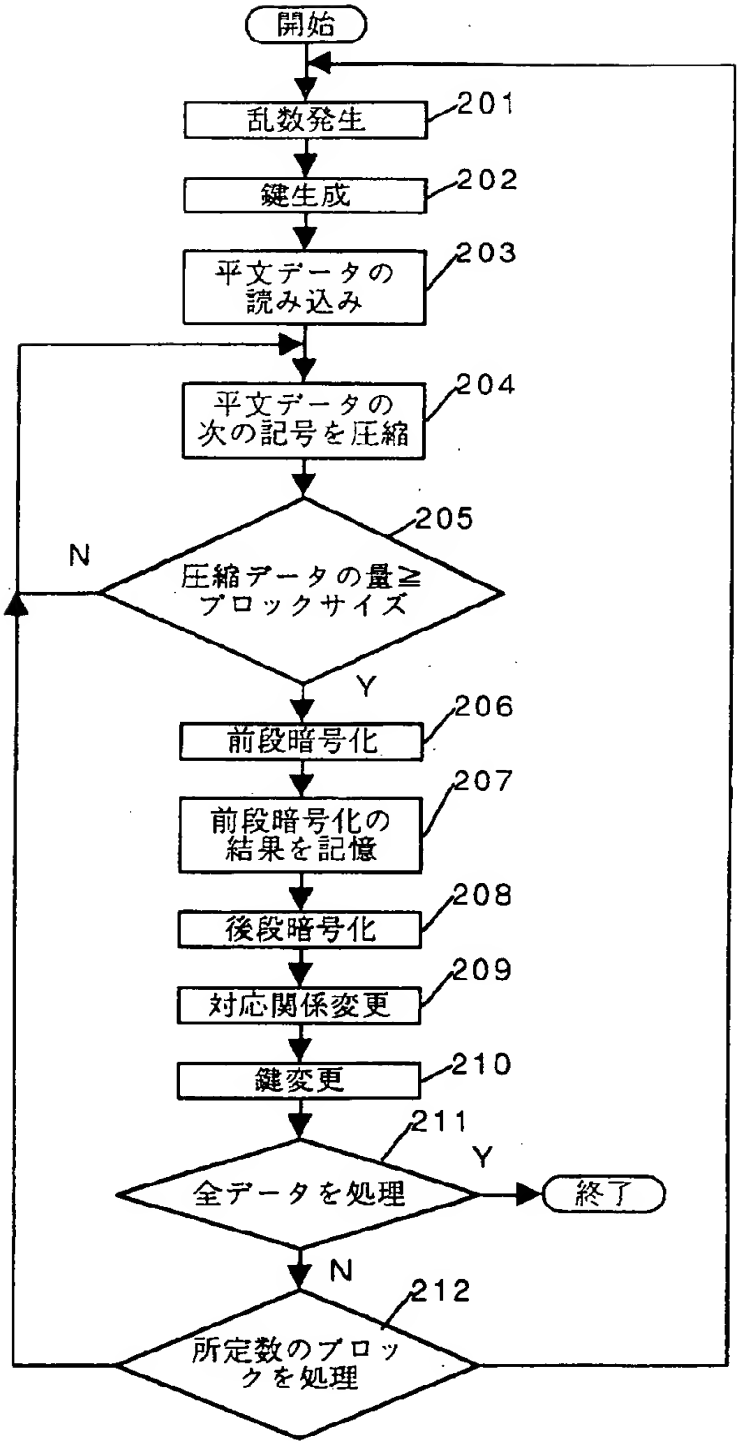


【図1】

図1


101
102
入出力
103
制御
104
乱数発生
105
鍵生成
106
対応関係変更
107
圧縮
108
前段暗号化
109
後段暗号化
110
111
平文データ
112
乱数
113
共通鍵
114
対応関係
115
実行鍵
116
圧縮・暗号データ

【図２】


開始
乱数発生
201
鍵生成
202
平文データの読み込み
203
平文データの次の記号を圧縮
204
圧縮データの量≧ブロックサイズ
205
N
Y
前段暗号化
206
前段暗号化の結果を記憶
207
後段暗号化
208
対応関係変更
209
鍵変更
210
全データを処理
211
Y
終了
N
所定数のブロックを処理
212

【図４】

図４